

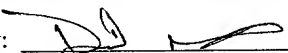
APPLICATION
FOR
UNITED STATES LETTERS PATENT

TITLE: **AN UNDETECTABLE FIREWALL**

APPLICANT: **David Izatt**

"EXPRESS MAIL" Mailing Label Number: EV019543675US

Date of Deposit: 1/24/02

By:  David Mixon

AN UNDETECTABLE FIREWALL

Background of Invention

Field of the Invention

[0001] The invention relates generally to computer security. More particularly, this invention relates to a computer security system that provides undetectable firewall protection.

Background Art

[0002] As society's dependence on computers increases, the importance of security for computers and their networks also increases. Threats such as hackers can shut down or damage large computer networks and cost significant amounts of money, resources, and time. Security measures to prevent such incidents are constantly evolving along with the nature and sophistication of the threat.

[0003] One technique to protect a computer network from external threats is by using a "firewall". A firewall is a combination of hardware and software that is placed between a network and its exterior. Figure 1 shows a schematic of a prior art network 10 with a firewall. The network 10 includes a series of users 12a – 12d that are linked and controlled through a server 14. The device could also be a router or a switch for the network. A firewall 16 is installed between the server 14 and the network exterior 20. The server 14, the firewall 16, and the exterior 20 are interconnected through a single line 18. The single line 18 prevents outsiders from accessing the network except through the firewall 16. The firewall receives all data from the network exterior before it is sent to the network users. The data may be e-mail, encrypted data, internet queries, or any other type of network traffic.

The firewall sorts and analyzes the data and determines whether it should have access to the network. If the data is authorized, the firewall forwards the data on to its destination. If the data is unauthorized, the firewall denies access to the network.

[0004] Data is normally transmitted in multiple bundles of information called “data packets” or “packets”. A message, query, etc. from the outside network is broken down into these packets in order to provide more efficient transmission of the data. Once all packets of data arrive at the destination, the packets are re-assembled. However, the packets contain more information than just the transmitted data. Figure 2 shows a diagram of a prior art data packet 30. The packet 30 includes three segments: a header 32; a body 34; and a trailer 36. The body 34 is the segment that contains the actual substance of the data.

[0005] The header 32 and the trailer 36 both contain various fields that are necessary for the administrative control of the packet 30. The header 32 segment includes: a flag 38a; an address field 40; and a control field 42. The trailer 36 segment includes: a sequence check field 44 and a flag 38b. The first flag 38a signifies the start of the packet 30. A second flag 38b signifies the end of the packet 30. The sequence check field 44 provides a check to ensure the data of the packet was properly received. The address field 40 includes the addresses of the source and the destination of the data. The control field 42 contains various information related to the administration of the packet 30 including a “time-to-live” field. The time-to-live field is an internal countdown mechanism that ensures that undeliverable or lost packets are deleted. The time-to-live field is given a certain value when the packet is first transmitted. As the packet passes through various servers, routers, switches, bridges, gateways, etc. that make up a network, the time-to-live field is decremented once by each device it passes through. Once the time-to-live field reaches zero, the packet is deleted. This

mechanism prevents a lost or undeliverable packet from circulating on the network in an endless loop.

[0006] Figure 3 shows a flow chart 50 of a prior art network firewall protection scheme. First, a packet is received at the firewall 52 from the network exterior 20. The firewall then conducts a handshake protocol 54 after receipt of the packet. The operations of network components are governed by protocols. A protocol is simply an established set of rules or standards that allow computers to connect with one another and exchange information and data with as little error as possible. Protocols may vary widely based different types of computer operating systems and on the different types of communications that are being transmitted. A handshake protocol governs a series of signals acknowledging that the transfer of data can take place between devices ("the handshake"). During the handshake, various changes are made to the packet by the firewall. The address of the firewall is added to the address field to show that the packet has left the firewall. Also, the time-to-live field is decremented by the firewall.

[0007] After completing the handshake 54, the packet is analyzed by the firewall to determine whether or not the data is acceptable to forward on to its destination in the network 56. The firewall analyzes the data through a technique called "pattern matching" that is well known in the art. Additionally, other techniques such as "protocol analysis" could be used as well. If the packet is authorized, it is forwarded on to the network destination by the firewall 58. If the packet is unauthorized, it is denied access to the network 60 and a message such as "resource denied" or "resource restricted" is sent to the sender. The party who sent the data from the exterior network is able to monitor and detect the presence of the firewall after the handshake protocol 62 and after access has been denied 62 due to the changes in the packet at the handshake 62. Once a hacker is able to detect the presence of a firewall, attempts can be made penetrate it and gain access to the network. If a hacker gains knowledge of the presence of a firewall, probes

can be made against it. Ultimately, the firewall may be breached or bypassed and unauthorized access to the network can be gained by the hacker.

[0008] In addition to the contents of the data packet described in Figure 2, a data packet will also contain an "ethernet frame field". The ethernet frame field is used by an ethernet card which is a piece of hardware within the firewall that manages access to the network. Figure 4 shows a schematic 70 of a prior art data packet with an ethernet frame field. The contents of the data packet are similar to what was previously described in Figure 2. The data packet includes three segments: a header 72; a body 74; and a trailer 76. The header 72 segment includes: a flag 78a; an address field 80; and a control field 82. The trailer 76 segment includes: a sequence check field 84 and a flag 78b. Additionally, two segments of the ethernet frame field 86a and 86b are included immediately in front of the first flag 78a and immediately following the second flag 78b respectively.

[0009] The ethernet frame field 86a and 86b is simply a protocol for processing the packet. Like the data packet, its contents are changed when it leaves the firewall. Specifically, the firewall adds its specific media access controller ("MAC") address to frame field 86a and 86b. The MAC address is a layer of the ISO/OSI (International Organization for Standardization/Open Systems Interconnection) reference model. The ISO/OSI model separates computer to computer communication into seven protocol layers. The ethernet card and the MAC are parts of one of the lower layers of this model and they manage access to the physical network.

[0010] One prior art solution is to make a firewall more difficult to detect (a "stealth firewall"). Figure 5 shows a flow chart 90 of a prior art network stealth firewall protection scheme. As shown previously in Figure 3, a packet is first received at the firewall 92 from the network exterior 20. However, a stealth firewall conducts a different type of handshake protocol 94. A stealth firewall

does not decrement the time-to-live field of the packet. Consequently, anyone monitoring the status of the packets in the network exterior 20 will not be able to see the stealth firewall due to a change in the value of the time-to-live field. After the stealth handshake 94, the stealth firewall analyzes the packet 96 in a similar manner as previously described for reference number 56 in prior art Figure 3. If the packet is authorized, it is forwarded on to the network destination by the firewall 98. If the packet is not authorized, it is denied access to the network 100. However, the firewall does not respond to the sender with any type of message indicating a denial of access. Instead, the stealth firewall simply drops the packet 102. The sender is prevented from detecting the stealth firewall by finding any indication of its presence in a decremented time-to-live field or a denial of access message.

[0011] However, a stealth firewall may still be detected by the changes it makes to the packet during its handshake protocol 94. Specifically, a stealth firewall leaves its own MAC address in the packet as it conducts the stealth handshake protocol 94. Once the presence of the stealth firewall is detected through the MAC address, a hacker can then begin to probe the firewall and attempt to find a way around it to gain access to the network. In order to prevent attacks by hackers on a firewall, it is necessary to make the firewall undetectable to parties outside the network.

Summary of Invention

[0012] In some aspects, the present invention relates to a method of preventing unauthorized access to a computer system, comprising: receiving a data packet at a firewall; copying the data packet at the firewall; analyzing the data packet with the firewall to determine if the data packet is authorized to access the computer system; sending an authorized data packet to the computer system; and denying access of an unauthorized data packet to the computer system.

[0013] In other aspects, the present invention relates to a method of preventing unauthorized access to a computer system, comprising: step of receiving data; step of passively copying the data; step of analyzing the data for authorization to access the computer system; and step of allowing access to the computer system for authorized data; and step of denying access to the computer system for unauthorized data.

[0014] In other aspects, the present invention relates to a method of remotely managing a firewall, comprising: receiving a control data packet at the firewall from a remote location; copying the control data packet at the firewall; analyzing the control data packet to determine if the control data packet is authorized to access the firewall; and allowing an authorized control data packet to control the firewall.

[0015] In other aspects, the present invention relates to a method of remotely managing a firewall, comprising: step of receiving control data at the firewall from a remote location; step of copying the control data; step of analyzing the control data to determine if the control data is authorized to access the firewall; and step of allowing authorized control data to access the firewall.

[0016] Other aspects and advantages of the invention will be apparent from the following description and the appended claims.

Brief Description of Drawings

[0017] Figure 1 shows a schematic of a prior art network with a firewall.

[0018] Figure 2 shows a schematic of a prior art data packet.

[0019] Figure 3 shows a flow chart of a prior art network firewall protection scheme.

- [0020] Figure 4 shows a schematic of a prior art data packet with an Ethernet frame.
- [0021] Figure 5 shows a flow chart of a prior art network stealth firewall protection scheme.
- [0022] Figure 6 shows a flow chart of one embodiment of network firewall protection in accordance with the present invention.
- [0023] Figure 7 shows a flow chart of an alternative embodiment of network firewall protection in accordance with the present invention.
- [0024] Figure 8 shows a firewall network with an external controller in accordance with one embodiment of the present invention.
- [0025] Figure 9 shows a flow chart of one embodiment of external network control of a firewall in accordance with the present invention.

Detailed Description

- [0026] An undetectable firewall for network protection has been developed. Figure 6 shows a flow chart 110 of one embodiment of network firewall protection in accordance with the present invention. First, a packet is received at the firewall 112 from the network exterior 20. The embodiment of the present invention conducts a "passive copying" 114 of the packet. After the packet is passively copied 114, the firewall analyzes the packet to determine whether or not it is acceptable to forward on to its destination in the network 116. The firewall analyzes the packet by the pattern matching technique, protocol analysis, or any other suitable technique that is known in the art. If the packet is acceptable, it is passed on through to the network 118. If the packet is not acceptable, access to the network is denied 120 and the packet is dropped 122 with no denial of access message being sent to the source of the packet. As a result, there is no detectable response to the sender of denied access from the firewall.

[0027] The passive copying 114 by the firewall of the packet is a low level operation that does not change the contents of the packet. No address exists for the firewall. Consequently, no address from the firewall is added to the packet, including the MAC address. Instead, the firewall allows the ethernet frame field along with the source address and other information of the packet to stay the same as when it was received by the firewall. The copied ethernet frame field is then used to transport the data packet. Additionally, the time-to-live field is not decremented by the firewall because the protocol of the operating system that requires decrementing is ignored. The entire contents of the packet, including the header with its address and control fields are exactly the same as when the packet was received by the firewall. Consequently, any party outside the network will not be able to detect the presence of the firewall by examining the contents of the packet or the ethernet frame field.

[0028] Figure 7 shows a flow chart 130 of an alternative embodiment of network firewall protection in accordance with the present invention. As in Figure 6, a packet is received at the firewall 132 from the network exterior 20. The embodiment of the present invention conducts a "passive copying" 134 of the packet. This passive copying is the essentially the same as described previously for Figure 6. After the packet is passively copied 134, the firewall analyzes the packet to determine whether or not it is acceptable to forward on to its destination in the network 136. The firewall analyzes the packet by the pattern matching technique, protocol analysis, or any other suitable technique that is known in the art. If the packet is acceptable, it is passed on through to the network 138. If the packet is not acceptable, access to the network is denied 140 and the packet is dropped 142 with no denial of access message being sent to the source of the packet. As a result, there is no detectable response to the sender of a denied from the firewall. Additionally, after the denial of access 140 and dropping the packet 142, the attempted intrusion into the network is logged 144. In alternative

embodiments, the logging could be done before or simultaneous to dropping the packet **142**.

[0029] The logging of the attempted access offers several possible actions available to network administrators. The logs of attempts of unauthorized access could be forwarded on to the authorities for further investigation. Also, if the packets are part of a “denial of service” attack, the data could be routed back to the attacker. Typically, a denial of service attack involves a multitude of requests to the network in such volume that it effectively shuts the network down.

[0030] In alternative embodiments, the firewall could be located in front of various segments of the network instead of only at the connection to the network exterior. This would provide protection not just from the network exterior, but also from other parts of the network. It also provides backup security should another firewall fail. The firewall could also be used to protect other network components such as routers and switches as well as the end users themselves.

[0031] In addition to protecting against unauthorized intrusion, the present invention may also be used to remotely control and manage the firewall. Figure 8 shows a firewall network with an external controller **150** in accordance with one embodiment of the present invention. The network **150** is similar to the prior art network previously described in Figure 1. The network **150** includes a series of users **152a – 152d** that are linked and controlled through a server **154**. The device could also be a router or a switch for the network. A firewall **156** is installed between the server **154** and the network exterior **20**. The server **154**, the firewall **156**, and the exterior **20** are interconnected through a single line **158**. The single line **158** prevents outsiders from accessing the network except through the firewall **156**. In addition, an external controller **160** is shown in the network exterior **20**. The controller **160** is used to remotely manage the firewall by a user such as a system administrator.

[0032] The controller 160 contacts the firewall 156 through the data line from the network exterior. The controller uses a technique known as “spoofing” to establish contact with the controller 160. Spoofing involves sending a transmission that appears to be coming from another source in order to hide the identity of the sender. Typically, this is done by embedding the address of the phony source in the data packet. In this embodiment of the invention, the controller 160 sends a command packet that is intended for the firewall 156 to some address destination behind the firewall. Inside the command packet is a password as well as command instructions to control the firewall 156. While a password is used in this embodiment, other embodiments could use other types of identification that are known in the art. Additionally, both the source address and the MAC address of the external controller 160 are spoofed to appear that they are coming from another source besides the external controller 160. Once the command packet is received at the firewall 156, the firewall conducts its passive copying of the packet and it searches for the password. If the password is found, the command packet is allowed to access the firewall 156. After access is allowed, the command data packet from the controller 160 is dropped without a trace.

[0033] Figure 9 shows a flow chart 170 of one embodiment of external network control of a firewall in accordance with the present invention. As in Figures 6 and 7, a packet is received at the firewall 172 from the network exterior 20. The embodiment of the present invention conducts passive copying 174 of the packet. This passive copying is the essentially the same as described previously for Figures 6 and 7. After the packet is passively copied 174, the firewall analyzes the packet to determine whether or not it is acceptable to forward on to its destination in the network 176. The firewall analyzes the packet by the pattern matching technique, protocol analysis, or any other suitable technique that is known in the art. If the packet is not acceptable, access to the network is denied 178 and the

packet is dropped **180** with no denial of access message being sent to the source of the packet. As a result, there is no detectable response to the sender of denied access from the firewall. In other embodiments, after the denial of access **178** and dropping the packet **180**, the attempted intrusion into the network could be logged as previously described in Figure 7. In alternative embodiments, the logging could be done before or simultaneous to dropping the packet **180**.

[0034] If the packet is authorized to access the network, it is examined for a password that indicates it is from the external controller **182**. If no password is found, the packet is sent on to its network destination **184**. If the password is found, the packet is allowed to access the firewall **186** and its command instructions are implemented. Finally, the packet is dropped by the firewall **188**. In alternative embodiments, the packet could be examined for the password of the external controller **182** either before or simultaneously with the analysis of the data for proper authorization **176** to access the network.

[0035] This technique of managing a firewall provides security for several reasons. First, the firewall leaves no trace of its presence in the command packet by passively copying its contents. Also, the external controller leaves no trace of its origin by spoofing its address. Additionally, the command packet hides its true destination because it appears to be addressed to a destination behind the firewall. Finally, after the command packet accesses the firewall and its command instructions are received, it is dropped without a trace. Consequently, the firewall and its control mechanisms are hidden from any unauthorized parties who may be monitoring or intercepting network traffic.

[0036] While the invention has been described with respect to a limited number of embodiments, those skilled in the art, having benefit of this disclosure, will appreciate that other embodiments can be devised which do not depart from the

scope of the invention as disclosed here. Accordingly, the scope of the invention should be limited only by the attached claims.